数理解析研究所講究録 1219 巻 2001 年 11-16

Diophantine equations over the twentieth century: a (very) brief overview

Yann Bugeaud

1. Introduction

The notion of variable, or unknown, first appeared in the works of the Greak mathematician Diophantus, who lived probably during the third century a.d. He considered polynomial equations with integral or rational coefficients, and was searching for an integral or rational solution. The most popular example is the equation $x^2 + y^2 = z^2$, whose integral solutions give us the lengths of the sides of Pythagorean triangles. At that time (and most probably since ever a few centuries), these were perfectly known.

Nowadays, we call Diophantine equation any polynomial equation with integer coefficients and whose unknowns are supposed to be rational integers. This definition is often extended to exponential equations, like Fermat's equation $x^n + y^n = z^n$, where x, y, z and $n \geq 3$ are unknown, however these are also sometimes called exponential Diophantine equations.

The natural question is the following: an equation being given, determine the set of its integral solutions. In most of the cases, this is far from being easy, and often this is even quite difficult to prove whether this set is finite or not. In the case of finiteness of the number of solutions, the second natural step is to try to compute an upper bound for their absolute values, or at least for their number. I emphasize that these two informations are absolutely not equivalent. Indeed, if we know that an equation has at most ten solutions, nothing ensures us that it has exactly ten solutions and while we have not found ten solutions we cannot be sure that we have completely solved the equation. However, if we manage to prove that all the solutions have at most, say, ten billions of digits, then, by enumerating all the possible solutions, we can, at least in principle (!), solve completely our equation. In the latter case, we know when we can stop our enumeration process, which is not the case when our informations only deal with the number of solutions.

Keeping in mind this essential feature of the Diophantine problems, we give in the sequel a short (and far from being complete) overview of the main achievements appeared during the twentieth century. For more informations, the reader is directed to the books [14, 15, 16, 18].

2. Ineffective methods

Apart from a result of Runge [12] dealing with a restricted family of Diophantine equations of the shape $F(x,y) = 0$, where $F \in \mathbf{Z}[X,Y]$ is a polynomial, we knew at the beginning of the twentieth century no general statement on the resolution of Diophantine equations. In 1909, the Norwegian mathematician Axel Thue [20] succeeded in proving that, for any homogeneous, irreducible polynomial $F \in \mathbf{Z}[X, Y]$ of degree at least 3, the equation (now called Thue equation)

$$F(x, y) = m, \tag{1}$$

where m is a given non-zero integer, has only finitely many solutions $(x, y) \in \mathbf{Z}^2$. The method of the proof allows us to compute an explicit bound for the number of solutions, but unfortunately not for their size. In the usual terminology, we say that Thue's result is *ineffective*, which means that it does not yield an effectively computable upper bound for the size of the solutions. One can further observe that the assumption on the degree of F is necessary, since Pellian equations may have infinitely many solutions.

Thue's result was completed in 1929 by a work of Siegel [17], who proved that, given a polynomial $F \in \mathbf{Z}[X, Y]$ such that the curve $F(x, y) = 0$ has genus one, the Diophantine equation $F(x, y) = 0$ has only finitely many solutions in integers x and y. As a corollary, the superelliptic equation

$$f(x) = y^m, \tag{2}$$

where $f \in \mathbf{Z}[X]$ is a polynomial of degree at least 2 and $m \geq 3$ is an integer, has only finitely many solutions $(x, y) \in \mathbf{Z}^2$. Like Thue's theorem, Siegel's result is ineffective. And all the extensions of their works, obtained notably by (among others) Mahler [11], suffer from the same inconvenience: the finiteness results are proved by ineffective methods... And we had to wait until the end of the sixties to see the development of a new and very powerful theory.

3. Baker's theory

In the fourties, Gelfond (see e.g. [9]) has obtained non-trivial explicit lower bounds for non-zero expressions of the shape

$$\Lambda = |b_1 \log a_1 + b_2 \log a_2|,$$

where a_1, a_2, b_1 and b_2 are non-zero algebraic numbers, which can be used to get explicit upper bounds for the solutions of certain Thue equations of degree 3. He also pointed out that a generalization of his result to linear forms in $m \geq 3$ logarithms would yield an effective upper bound for the size of the solutions of any Thue equation of degree arbitrarily large.

Such a generalization has been proved by Alan Baker [1] in 1966 and refined in several subsequent works (see [4] for references). This enabled Baker to compute [2, 3], for the first time, explicit (huge) upper bounds for the size of the solutions of (1) and (2), and also, jointly with Coates [5], to give an explicit version of Siegel's theorem quoted above.

Apart from this aspect, the theory of linear forms in logarithms appears to be much more powerful than the methods developed by Thue and Siegel. Indeed, it also applies to certain families of exponential Diophantine equations (recall that this terminology means that one or several exponents are unknown), like for instance

$$f(x) = y^q, \tag{3}$$

where $f \in \mathbf{Z}[X]$ is a given irreducible polynomial of degree at least 3 and x, y and $q \geq 2$ are unknown integers. Baker's theory enables us to compute an explicit upper bound for the size of the largest solution of (3), while Thue–Siegel's method appears to be useless.

The most spectacular achievement, maybe, was obtained by Tijdeman [21] in 1976. He proved that Catalan's equation

$$x^m - y^n = 1, \tag{4}$$

in integers x, y, m and n at least equal to 2, has only finitely many solutions, whose size can be explicitely bounded. Indeed, following Tijdeman's proof and using the estimates for linear forms in logarithms available at that time, Langevin has computed that for any solution (x, y, m, n) of (4) one has

$$\max\{x, y, m, n\} \leq \exp\exp\exp\exp 730.$$

Roughly speaking, the situation twenty years ago was the following : we were able to compute explicit upper bounds, but these were far too huge in order to solve completely the equations considered.

4. Nowadays

These last years, numerous spectacular results have been proved, which seemed, even ten years ago, to be far beyond our possibilities. There are two main explanations. The first one concerns a theoretical improvement: the size of the numerical constants appearing in the estimates for linear forms in logarithms has been substantially reduced and is now (at least in the case of two logarithms) rather satisfactory. The second one is the development of the algorithmic number theory, one of the most dynamic branches of the current mathematics.

For instance, we have now at our disposal efficient algorithms which enable us to solve any Thue equation of small degree, say of degree less than twenty, and with small coefficients. Further, there are examples of equations of high degree which are completely solved. The following one, due to Hanrot [10], is quite impressive.

Theorem 1. *The Diophantine equations*

$$\prod_{1 \leq k \leq 2000} \left(Y - 2\cos\left(\frac{2\pi k}{4001}\right) X \right) = \pm 1, \pm 4001 \tag{5}$$

have no non-trivial integral solutions.

I should however point out that this absolutely does not mean that we are now able to solve any Thue equation of degree less than two thousand! One should be aware that (5) has a very particular shape: the right-hand side is indeed a cyclotomic polynomial.

In 1976, Shorey & Tijdeman (see for instance Chapter 12 of [16]) proved in an effective way that only finitely many integers greater than 2 of the form $11\ldots11$, i.e. with only the digit 1, can be pure powers. This was the first step towards a proof of a longstanding conjecture claiming that none of these numbers is a pure power, which has recently been settled by Bugeaud & Mignotte [7].

Theorem 2. *Excepted 1, no integer with only the digit 1 in base ten can be a pure power.*

The original proof uses sharp estimates for linear forms in two non-Archimedean logarithms, as well of a great amount of computer calculations. Some of them could be avoided by application of the beautiful Theorem 3 (due to Bennett [6]) below... which, however, also requires a lot of computer calculations (but not the same ones!).

Theorem 3. *Let $a > b \geq 1$ and $n \geq 3$ be integers. Then the Diophantine equation*

$$|ax^n - by^n| = 1$$

has at most one solution in positive integers x and y.

5. Results from arithmetic geometry

A common feature of all the results mentioned above is that they belong to the area usually called "Diophantine approximation". Motivated in part by Fermat's conjecture, another branch of mathematics, sometimes named arithmetic geometry, appeared in the middle of the twentieth century. Many mathematicians have contributed to its development, and here are (only) two of their main achievements.

The first one is due to Faltings [8], who proved in 1983 that there are only finitely many rational points on every curve of genus at least two defined over the rationals. Notice that Falting's result deals not only with integral points but also with rational ones. It solves a conjecture of Mordell and provides a generalization of the result of Siegel quoted in Section 2. However, there is at present time no effective version of Faltings' theorem, while, as mentioned in Section 3, Baker & Coates proved effectively that there are only finitely many integral points on a curve of genus one defined over the rationals. Falting's proof uses deep tools of arithmetic geometry and algebraic geometry, however, alternative proofs, depending more on classical methods in Diophantine approximation, have been given by Vojta and Bombieri.

The second spectacular achievement is of course Wiles' theorem [19, 22] that there is no solution in positive integers x, y, z and $n \geq 3$ to the equation $x^n + y^n = z^n$. The proof is very difficult and extremely ingenious. Later, similar ideas have been used to solve completely several equations of the shape $x^n + y^n = cz^n$, where c is a fixed positive integer. However, it seems that when one wants to find all the solutions of a given Diophantine equation, methods arising from Diophantine approximation are, very often, much more efficient than methods from arithmetic geometry...

6. One (big) omission

I will only point out one of the many applications of Schmidt's Subspace Theorem and its recent versions. The main raison for which I have omitted such a powerful tool is that this yields, at present time, only ineffective results and does not help for the complete resolution of Diophantine equations. Let S denote the set of integers whose prime factors belong to $\{2,3,5\}$. Let $n \geq 2$ be an integer, and consider the equation

$$u_1 + \ldots + u_n = 1, \tag{6}$$

in unknowns $u_i \in S$. The subspace theorem tells us (see for instance [15], Chapter V) that (6) has only finitely many solutions $(u_1, \ldots, u_n)$ such that no subsum $u_{i_1} + \ldots + u_{i_k}$ vanishes. Further, we are able to state explicitely an upper bound for the number of solutions of (6), but unfortunately not for their size (excepted however when $n = 2$, where Baker's theory can be applied).

7. One open problem

Many interesting open problems remain, but I choose to quote only one of them, namely a question appeared in a work of Schinzel & Tijdeman [13].

Problem. *Let $f \in \mathbf{Z}[X]$ be an irreducible polynomial of degree at least 2. Do the Diophantine equation*

$$f(x) = y^2 z^3$$

have only finitely many solutions in non-zero integers x, y and z ?

It is very likely that completely new ideas are required to give an (even partial) answer to that question.

Acknowledgement: I would like to express my deep thanks to Leo Murata and Isao Wakabayashi. The conference was perfectly organized and its atmosphere was very friendly.

References

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 12 (1966), 204-216.

[2] A. Baker, *Contributions to the theory of diophantine equations.* I, *On the representation of integers by binary forms.* II, *The diophantine equation $y^2 = x^3 + k$*, Phil. Trans. R. Soc. London A 263 (1968), 173-208.

[3] A. Baker, *Bounds for the solution of the hyperelliptic equation*, Proc. Camb. Phil. Soc. 65 (1969), 439-444.

[4] A. Baker, Transcendental Number Theory, Cambridge Univ. Press, 1975.

[5] A. Baker and J. Coates, *Integer points on curves of genus 1*, Proc. Camb. Phil. Soc. 67 (1970), 595–602.

[6] M. Bennett, *Rational approximation to algebraic number of small height : The diophantine equation* $\mid ax^n - by^n \mid= 1$, J. reine angew. Math., to appear.

[7] Y. Bugeaud and M. Mignotte, *On integers with identical digits*, Mathematika, to

[8] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[9] A. O. Gelfond, Transcendental and algebraic numbers, Dover publ., New York, 1960.

[10] G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp. 69 (1999), 395–405.

[11] K. Mahler, *Zur Approximation algebraischer Zahlen, I. Ueber den grössten Primteiler binärer Formen*, Math. Ann. 107 (1933), 691-730.

[12] C. Runge, *Ueber ganzzahlige Lösungen von Gleischungen zwischen zwei veränderlichen*, J. Reine Angew. Math. 100 (1887), 425-435.

[13] A. Schinzel and R. Tijdeman, *On the equation $y^m = f(x)$*, Acta Arith. 31 (1976), 199–204.

[14] W. M. Schmidt, Diophantine Approximation, Lecture Notes in Math. 785, Springer, Berlin, 1980.

[15] W. M. Schmidt, Diophantine Approximations and Diophantine equations, Lecture Notes in Math. 1467, Springer, Berlin, 1991.

[16] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations, Cambridge Tracts in Mathematics 87 (1986), Cambridge University Press, Cambridge.

[17] C. L. Siegel, *Ueber einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-math. Kl. 1 (1929), 41-69.

[18] V. G. Sprindžuk, Classical Diophantine Equations, Lecture Notes in Math. 1559, Springer-Verlag, Berlin, 1993.

[19] R. Taylor and A. Wiles, *Ring–theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553–572.

[20] A. Thue, *Ueber Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. 135 (1909), 284-305.

[21] R. Tijdeman, *On the equation of Catalan*, Acta Arith. 29 (1976), 197–209.

[22] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141 (1995), 443–551.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG (France)

e-mail : `bugeaud@math.u-strasbg.fr`